UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	Criminal Action
v.	)	No. 21-10104-PBS
	)	
VLADISLAV KLYUSHIN,	)	
	)	
Defendant.	)	

MEMORANDUM AND ORDER

December 2, 2022

Saris, D.J.

INTRODUCTION

A grand jury indicted Russian national Vladislav Klyushin for allegedly hacking into American computer systems and using the confidential information he obtained to make profitable trades in the shares of public companies. The Indictment states four counts against Klyushin and his alleged co-conspirators Ivan Ermakov and Nikolai Rumiantcev: (I) Conspiracy, (II) Wire Fraud, (III) Unauthorized Access to Computers, and (IV) Securities Fraud. Klyushin now moves to dismiss Count IV of the Indictment and to partially dismiss Count I as to the allegations of conspiracy to commit securities fraud. Klyushin further asks the Court to suppress evidence the government seized pursuant to search warrants. After hearing, the Court **DENIES** the motion to dismiss and **DENIES** the motion to suppress.

FACTUAL BACKGROUND

A. The Indictment

The Indictment alleges the following facts.

Klyushin was the owner and first deputy general director of M-13, a purported information technology company in Moscow. Ermakov and Rumiantcev were deputy general directors of M-13. M-13 offered technological and media monitoring services to enterprises and government entities in Russia, including testing and analyzing organizations' cybersecurity preparedness. M-13 also offered investment management services to at least three individuals in exchange for up to 60 percent of the profits.

From approximately January 2018 through September 2020, Klyushin, Ermakov, and Rumiantcev schemed to gain access to information stored on the computer networks of two American filing agents ("Filing Agent 1" and "Filing Agent 2"), then traded on the information for profit. Filing agents assist public companies with their SEC filings. Consequently, they frequently possess the quarterly and annual financial data of public companies before they become public. Klyushin, Ermakov, Rumiantcev, and their co-conspirators operated malicious software to steal the usernames and passwords of employees of Filing Agents 1 and 2, and then used the credentials to log into the Filing Agents' computer networks. Once inside the Filing Agents' networks, the defendants and their co-conspirators viewed or downloaded the financial disclosures of

publicly traded companies and used the data to make profitable trades on securities exchanges.

On January 21, 2020, Ermakov used the login credentials of an employee of Filing Agent 1 to access the quarterly earnings information of Avnet, Inc., whose securities trade on the NASDAQ. Two days later, Ermakov used Klyushin's account at a Denmark-based bank to take a short position in Avnet securities, betting that their value would fall. Another co-conspirator also shorted Avnet shares. Hours after these trades, Avnet reported disappointing quarterly financial results.

The Indictment recites additional specific examples of the co-conspirators using employee login credentials to access the Filing Agents' computer networks and trading on public company financial information they found.

B. The Search Warrants

The government seized evidence pursuant to a search warrant directed to Apple, Inc. on September 29, 2020 (the "September 29 Search Warrant") and search warrants directed to Apple, Inc. and Google, LLC on October 13, 2020 (the "October 13 Search Warrants"). The government based its search warrant applications on two affidavits of FBI Special Agent BJ Kang (the "September 29 Affidavit" and the "October 13 Affidavit"). In the September 29 Affidavit, the government sought to search the email address MIKKA777@yahoo.com, belonging to another target of the

investigation, Mikhail Irzak, and Klyushin's Apple iCloud account associated with the email address 9227748@gmail.com. The October 13 Affidavit was in support of applications to search the Apple iCloud account associated with the Apple ID 1093366326 and the Google account 9227748@gmail.com, both linked to Klyushin. The two affidavits are substantially similar, and the Court will recite the facts they aver while noting any material differences.

The affidavits discuss the allegedly unlawful trading activities of various of the targets, focusing on Irzak and Klyushin. In September 2019, the SEC informed the FBI that it had identified a group of traders, including Irzak, who had made suspicious trades in the shares of several publicly traded companies before their earnings announcements. Approximately 95% of the companies whose shares the traders purchased or sold used Filing Agent 1 or Filing Agent 2 to assist with their quarterly filings. On January 16, 2020, the Financial Industry Regulatory Authority notified the SEC that in October and November, 2019, a client account at Otkritie Broker, Ltd., a Cyprus-based brokerage firm headquartered in Russia, had made profitable trades in the immediate leadup to 21 quarterly earnings announcements. Irzak traded in parallel with many of this account's trades. In early 2020, the FBI learned that Filing Agent 1 and 2's computer networks and employee login credentials were compromised. Through the

Filing Agent 1 hack, Avnet's earnings data was exposed on January 21, 2020.

The affidavits tie Klyushin to the scheme through Ermakov's Avnet trades. Ermakov had been indicted in the District of Columbia for interference in the 2016 United States elections and in the Western District of Pennsylvania for hacking into the servers of various sporting and anti-doping agencies. Special Agent Kang's review of Ermakov's Apple account showed that Ermakov had access to an account belonging to Klyushin on the SaxoTraderGO app[1] and that the account had images of Avnet "contracts for difference" dated January 23, 2020.[2] Irzak and other overseas traders sold Avnet shares short on the same day. The September 29 Affidavit (but not the October 13 Affidavit) also states that Klyushin's Saxo trading account "is believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earning's announcements." Dkt. 98 ¶ 38. At the hearing, the government could not explain why the statement was struck from the October 13 Affidavit.

Special Agent Kang found that Ermakov listed Klyushin's phone

[1] The app is a mobile trading platform for Saxo Bank clients. The September 29 Affidavit describes Saxo Bank as "a Danish-based investment bank that specializes in online trading and investment." Dkt. 98 ¶ 29.

[2] A contract for difference is an agreement that allows traders to speculate as to the future movement of a stock price.

as a contact. He also learned that Klyushin was associated with the 9227748@gmail.com address and that Ermakov and Klyushin had corresponded over WhatsApp on many occasions between May 29, 2020 and July 9, 2020. Ermakov had an entry on his Apple calendar that indicated he had a meeting with "Vlad" about the stock exchange. Dkt. 98 ¶ 40; Dkt. 98-2 ¶ 25. Special Agent Kang believed the "Vlad" may have been a reference to Klyushin.

The Magistrate Judge issued the September 29 Search Warrant authorizing the FBI to search Klyushin's Apple iCloud account associated with the email address 9227748@gmail.com. Review of the Apple-produced records showed that this account was locked but that Klyushin's phone was associated with the Apple ID 1093366326. Accordingly, the FBI submitted the October 13 Affidavit. The Magistrate Judge issued the October 13 Search Warrants, which authorized the FBI to search both the iCloud account with the Apple ID 1093366326 and the 9227748@gmail.com Google account. The warrant to Apple listed 19 categories of evidence as examples of the types of information the FBI could search and seize pursuant to the warrant.

DISCUSSION

A. Motion to Dismiss[3]

Klyushin seeks dismissal of Count IV of the Indictment,

[3] The Court denied the motion to dismiss at the October 31, 2022 hearing, and elaborates upon its reasoning for the denial below.

alleging securities fraud, and so much of Count I as alleges a conspiracy to commit securities fraud. An indictment "must be a plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c)(1). The Court presumes that the allegations of the indictment are true in assessing a motion to dismiss. See United States v. Dunbar, 367 F. Supp. 2d 59, 60 (D. Mass. 2005).

Count IV of the Indictment alleges that Klyushin violated Section 10(b) of the Securities Exchange Act of 1934 and the SEC's Rule 10b-5. These two provisions prohibit fraud in the purchase or sale of securities. Section 10(b) makes it unlawful

> for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange . . . [t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

15 U.S.C. § 78j(b).

Rule 10b-5 is the primary implementing regulation of Section 10(b), and makes it unlawful, in connection with the purchase or sale of any security,

> for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange, (a) To employ any device, scheme, or artifice to defraud, (b) To make any untrue statement of a material fact or to omit to state a material fact

> necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

17 C.F.R. § 240.10b-5.

The question before the Court is whether a hack-and-trade scheme like that alleged in the Indictment amounts to securities fraud. The parties agree that the Second Circuit is the only court of appeals to have addressed this question. Its holdings directly support the government's position that hacking into computer systems to obtain and trade on material, nonpublic information ("MNPI") is securities fraud. See S.E.C. v. Dorozhko, 574 F.3d 42, 50–51 (2d Cir. 2009); see also United States v. Khalupsky, 5 F.4th 279, 290–91 (2d Cir. 2021), cert. denied sub nom. Korchevsky v. United States, 142 S. Ct. 761 (2022).

Klyushin argues that he cannot be liable for securities fraud because he did not have a fiduciary duty to the companies he took information from or those whose securities he traded in. Dorozhko and Khalupsky squarely reject this argument's application in the context of a hack-and-trade scheme. See Dorozhko, 574 F.3d at 49 ("Even if a person does not have a fiduciary duty to disclose or abstain from trading, there is nonetheless an affirmative obligation in commercial dealings not to mislead.") (internal quotation marks omitted); Khalupsky, 5 F.4th at 290 ("Although a fiduciary duty is relevant to other securities violations -- e.g.,

insider trading -- it need not be shown to prove the securities fraud charged here: fraudulent trading in securities by an outsider."). Consistent with this caselaw, this Court holds that affirmatively misrepresenting one's identity to access, steal, and trade on confidential information is deceptive within the meaning of Section 10(b) and Rule 10b-5. Klyushin's motion to dismiss is therefore denied.

B. Motion to Suppress[4]

1. Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In reviewing a probable cause determination, the Court gives "significant deference to the magistrate judge's initial evaluation" and reverses only if there is "no 'substantial basis' for concluding that probable cause existed." United States v. Ribeiro, 397 F.3d 43, 48 (1st Cir. 2005) (quoting United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999)). "A warrant application must establish probable cause to believe that (1) a crime has been committed --

[4] The government represents that it does not intend to admit evidence from the Google account 9227748@gmail.com. The Court will deny as moot Klyushin's motion to suppress evidence obtained from that account. The Court's suppression analysis concerns Klyushin's Apple accounts.

the 'commission' element, and (2) enumerated evidence of the offense will be found at the place to be searched -- the so-called 'nexus' element." United States v. Bregu, 948 F.3d 408, 414 (1st Cir. 2020) (cleaned up). Assessing whether an affidavit supports a finding of probable cause requires making a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit" there is "a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Tanguay, 787 F.3d 44, 50 (1st Cir. 2015) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

Here, there was probable cause for the warrants to search Klyushin's Apple accounts. Special Agent Kang's affidavits connect the dots from Irzak to Ermakov to Klyushin, showing that there was a fair probability that evidence of a hack-and-trade scheme would be found in Klyushin's iCloud account. See United States v. Adams, 971 F.3d 22, 32 (1st Cir. 2020). The affidavits show that (1) there was an ongoing scheme, in which Irzak participated, that involved hacking into the Filing Agents' computer networks to obtain and trade on MNPI, including Avnet's MNPI; (2) Ermakov, a known hacker, had also traded in Avnet on the day of its earnings announcement; and (3) Ermakov had used Klyushin's account to make the Avnet trades and had corresponded with Klyushin repeatedly via phone in the months after the Avnet trades. A commonsense evaluation of these facts indicates that a

fair probability existed that Klyushin's iCloud account would contain evidence of the Avnet trades as part of the hack-and-trade scheme. Once the fruits of the September 29 Search Warrant showed that Klyushin's initial iCloud account was locked but that his phone was associated with the Apple ID 1093366326, there was also probable cause to search that second iCloud account.

Klyushin argues that the affidavits do not adequately tie him to a broad hack-and-trade scheme. He takes particular issue with Special Agent Kang's statement in the September 29 Affidavit that Klyushin's Saxo trading account "is believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earning's announcements." Dkt. 98 ¶ 38. The Court agrees that this statement is too vague (who "believed" it? On what basis?) to support a finding of probable cause. See United States v. Vigeant, 176 F.3d 565, 571 (1st Cir. 1999) (holding that "unsupported conclusions are not entitled to any weight in the probable cause determination."). Nonetheless, the Court finds that the other supported assertions in the affidavits, and particularly Ermakov's use of Klyushin's account to trade in Avnet shares in parallel with Irzak, suffice to establish probable cause to search Klyushin's iCloud accounts for evidence of the hack-and-trade scheme.

Even if there were no probable cause, suppression is unwarranted because the good faith exception to the exclusionary

rule would apply. Under the good faith exception, the government may use evidence obtained pursuant to a later-invalidated warrant if it acted with objective good faith based on a probable cause determination issued by a neutral and detached magistrate. See United States v. Leon, 468 U.S. 897, 920 (1984). The First Circuit has delineated the boundaries of the good-faith exception:

> Suppression remains appropriate:
> 1. If the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth.
> 2. Where the issuing magistrate wholly abandoned his judicial role.
> 3. Where the executing officer relies on a warrant based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.

United States v. Levin, 874 F.3d 316, 322 (1st Cir. 2017) (internal punctuation omitted) (quoting Leon, 468 U.S. at 923).

The government proffers that Special Agent Kang believed that Klyushin's account had traded in parallel with Irzak because the SEC sent him a spreadsheet evidencing such parallel trades. While the spreadsheet is not incorporated into the affidavits and does not bear on the probable cause analysis, it is relevant to Special Agent Kang's good faith. Thus, even if (contrary to the Court's finding) there were no probable cause for the search warrants, the good faith exception would apply and suppression would be inappropriate.

2. Particularity

To satisfy the Fourth Amendment's particularity requirement, a warrant "(1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized." United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013). The purpose of this requirement is "to prevent wide-ranging general searches by the police." United States v. Moss, 936 F.3d 52, 58 (1st Cir. 2019) (quoting United States v. Bonner, 808 F.3d 864, 866 (1st Cir. 1986)). A court must review the warrant's language as a whole in determining whether the warrant satisfies the particularity requirement. See Kuc, 737 F.3d at 133.

The warrants in this case each authorize law enforcement to search and seize information for the period January 1, 2018 to the time of search that constitute evidence of six offenses: wire fraud, conspiracy to commit wire fraud, fraud and related activity in connection with computers, money laundering and conspiracy to commit money laundering, securities fraud, and conspiracy to commit securities fraud. The Apple warrants then list nineteen examples of records that are among the types of evidence the government may search and seize. These categories include information related to MNPI of public companies; any relationship between the alleged participants in the scheme, including Irzak,

Klyushin, and Ermakov; Saxo Bank and other banks; intrusions into public networks; and filing agents for public companies. Other courts in this district have held that this structure satisfies the particularity requirement. See, e.g., United States v. Kanodia, No. 15-cr-10131-NMG, 2016 WL 3166370, at *5 (D. Mass. June 6, 2016); United States v. Tsarnaev, 53 F. Supp. 3d 450, 456–57 (D. Mass. 2014).

Klyushin argues that the warrants are overbroad because they (1) use non-exhaustive prefatory language describing the offenses at issue and the examples of documents to be seized, and (2) authorize the search of his iCloud account, which contains huge amounts of personal and irrelevant information. Even if the nineteen categories are broadly phrased, the language of the paragraphs must be read in context of the crimes at issue. See Kuc, 737 F.3d at 133–34. Indeed, a warrant need only provide reasonable specificity as to the categories of documents to be searched. See Archer v. Chisholm, 870 F.3d 603, 616 (7th Cir. 2017) ("[The investigating officer] could not know *ex ante*, with pinpoint specificity, what documents and e-mails existed.").

It is true that the search warrants directed Apple to broadly turn over to the government an iCloud account that contained substantial details of Klyushin's personal life that went beyond the temporal and substantive scope of the categories in the search warrants. However, the warrants only authorized the government to

search for specific categories of information from that seized account.[5] The fact that the government was authorized to search an iCloud account produced by Apple does not violate the Fourth Amendment so long as the search is consistent with the warrant. See Fed. R. Crim. P. 41(e)(2)(B).

"Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." Riley v. California, 573 U.S. 373, 393, 397 (2014) (noting that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity."). That a digital seizure of such immense storage capacity will reveal files containing irrelevant information is hardly novel, however, as "traditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are." United States v. Ulbricht, 858 F.3d 71, 100 (2d Cir. 2017), abrogated on other grounds by Carpenter v. United States, 138 S. Ct. 2206 (2018). Here, it suffices that the warrants direct law enforcement to particular places to be searched (i.e., Klyushin's iCloud accounts), the time period of the

[5] In this context, the seizure of the documents from Apple came first, and the search second.

documents to be searched, the offenses at issue, and the nineteen examples of records to be searched.

Klyushin complains bitterly that the government seized and used personal information that falls outside the warrant's scope, for example, at the bail hearing. One magistrate judge has required that a cloud storage provider like Apple conduct some degree of pre-production triage to filter out irrelevant documents. See In re. Search of Info. Associated with [redacted]@mac.com, 25 F. Supp. 3d 1, 8 (D.D.C. 2014). The government has sometimes used its own filtration teams to weed out privileged materials. See United States v. Aboshady, 951 F.3d 1, 5 (1st Cir. 2020) (authorizing Google to turn over an entire Gmail account, followed by a filtration team review and then review by the investigative team). Both of these procedures make sense. However, Klyushin does not argue that these procedures are constitutionally required, and no cited caselaw supports such a requirement. See United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (holding that the Fourth Amendment does not require the government to delegate a pre-screening function to the internet service provider). In any case, the remedy for an improper use of documents beyond the scope of the categories would be partial suppression of the unwarranted documents, not blanket suppression. See Aboshady, 951 F.3d at 9. Moreover, the

government has agreed not to use any documents prior to 2018 at trial.

3. Franks Hearing

An affidavit in support of probable cause is presumed valid. See Franks v. Delaware, 438 U.S. 154, 171 (1978). To obtain a hearing into an affiant's credibility, the defendant must make "a substantial preliminary showing that both (1) a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit and (2) the allegedly false statement is necessary to the finding of probable cause." United States v. Reiner, 500 F.3d 10, 14 (1st Cir. 2007) (cleaned up). An omission of information may also trigger a Franks hearing where the information is material. See United States v. Castillo, 287 F.3d 21, 25 (1st Cir. 2002). Where the defendant makes allegations that the affiant made a knowing or reckless falsehood, "those allegations must be accompanied by an offer of proof." Franks, 438 U.S. at 171.

Klyushin seeks a Franks hearing because the affidavits in support of probable cause did not disclose that a federal judge had cast doubt on Special Agent Kang's credibility in a previous insider trading case. Judge Holwell of the Southern District of New York found that Special Agent Kang made "misleading" and "literally false" statements in an affidavit in support of probable cause. United States v. Rajaratnam, No. 09-cr-1184, 2010 WL

4867402, at *10 (S.D.N.Y. Nov. 24, 2010). The affidavit failed to note that a cooperating witness had pleaded guilty to participating in a different insider trading scheme six years earlier -- a fact that could have cast doubt on the witness's credibility. See id. Moreover, the government had tried and failed in the same earlier case to establish insider trading by the defendant Rajaratnam, suggesting that it had been investigating him for years before the affidavit disclosed. See id. The court additionally found that Special Agent Kang had paraphrased certain phone conversations inaccurately. See id. at *10-*11. Finally, Judge Holwell faulted the government for failing to divulge that its criminal investigation had substantially relied on an SEC insider trading investigation into Rajaratnam, calling into question whether the wiretap at issue was necessary. See id. at *1. The court ordered a Franks hearing that only concerned whether the wiretap was necessary given the government's "reckless[]" failure to disclose the SEC investigation, but ultimately declined to suppress evidence after finding the omission immaterial. Id. at *1. On appeal, the Second Circuit reversed much of the district court's rulings on the falsity of Special Agent Kang's affidavit, finding that his omission of evidence regarding the SEC investigation had not occurred with "reckless disregard for the truth" and thus was not improper. United States v. Rajaratnam, 719 F.3d 139, 154-56 (2d Cir. 2013).

Here, binding precedent forecloses the possibility of a Franks hearing. In United States v. Southard, the First Circuit rejected the argument that a Franks hearing was warranted only because the district court had, in a prior related case, suppressed evidence following a Franks hearing arising from the same F.B.I. agent's affidavit. See 700 F.2d 1, 9-10 (1st Cir. 1983) (finding previous Franks hearing outcome "casts a certain degree of doubt upon" the affiant's credibility but nonetheless "proves nothing about the veracity of the affidavit at issue in this case and standing alone cannot establish appellants' right to a Franks hearing.").

Klyushin's argument in support of a Franks hearing relies entirely on the omission of Judge Holwell's critical statements - - which did not even result in the suppression of evidence in the Rajaratnam case. Without more, Klyushin is not entitled to a Franks hearing. Klyushin also has not shown how the alleged omission negates the Magistrate Judge's probable cause finding. He argues that it discredits Special Agent Kang's statement in the September 29 Affidavit that Klyushin's account was believed to have traded "in parallel" with Irzak. While the reason for the later omission of that assertion is unclear, the statement was not necessary to a finding of probable cause. Moreover, in light of the information from the SEC, there is no

reasonable inference of bad faith. Thus, Klyushin is not entitled to a Franks hearing.

ORDER

For the foregoing reasons, Klyushin's Motion to Dismiss (Dkt. 96) and Motion to Suppress (Dkt. 97) are **DENIED**.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge